A Model for Hybrid Evidence Investigation

K. Vlachopoulos, E. Magkos and V. Chrissikopoulos

Department of Informatics, Ionian University
Plateia Tsirigoti 7, 49100, Corfu, Greece
e-mail: {kostasv, emagos, vchris}@ionio.gr

Abstract

With the advent of Information and Communication Technologies, the means of committing a crime and the crime itself are constantly evolved. In addition, the boundaries between traditional crime and cybercrime are vague: a crime may not have a defined traditional or digital form since digital and physical evidence may coexist in a crime scene. Furthermore, various items found in a crime scene may worth be examined as both physical and digital evidence, which we consider as *hybrid evidence*. In this paper, a model for investigating such crime scenes with hybrid evidence is proposed. Our model unifies the procedures related to digital and physical evidence collection and examination, taking into consideration the unique characteristics of each form of evidence. Our model can also be implemented in cases where only digital or physical evidence exist in a crime scene.

Keywords

Physical forensics, digital forensics, crime investigation models, hybrid evidence

1. Introduction

Crime is an undisputable part of every society. During the centuries crime has been developed and so did crime investigation techniques. In the 20th century the need for investigating crime in a more accurate way has introduced forensic science, focusing on the collection and examination of evidence connected to a crime. In the 80's-90's the proliferation of computing and Internet technologies has broadened the means of committing a crime. Nowadays, the majority of conventional crime investigations face the need to search for extra evidence that may have been stored in digital form or been produced by digital devices. For example, offenders of the -so called- traditional crimes, like homicides or rapes, may have used the Web, e-mail, or cellular communication services to collect and transfer information related to the crime. Examining this evidence can for example produce valuable information about a crime, the motives of the offenders, the relationship between the offender and the victim, the accomplices of the offender. As a result, digital forensics flourished, becoming the key player in the battle against crime. (Reith *et al.*, 2002; Palmer, 2002; Vlachopoulos, 2007; Beebe, 2009; Garfinkel, 2010; Agarwal *et al.*, 2011).

In this cyber-physical environment it becomes extremely difficult to collect every single scratch of evidence or to find a specific piece of evidence. In the digital investigation field for example, a number of challenges need to be studied and

addressed (Sheldon, 2005; Beebe, 2009; Garfield, 2010), including: The decreasing size of storage devices which makes the creation of a forensic image or the processing of the data they contain, challenging; the expansion of malware stored in RAM that demands the development of specialized RAM forensics tools; the proliferation of smartphones and pervasive computing technologies that extend the need to search for evidence in a variety of new digital devices or physical items with embedded systems-on-chip (SOC), *e.g.*, clothes; the use of cloud computing technologies so that evidence cannot be found in a single computer or network and may be stored and/or processed outside the legal jurisdiction; legal issues related to security and privacy that influence both physical and digital investigation and the admissibility of collected evidence.

Particularly with the advent of smart environments, more and more everyday processes will be supported by pervasive devices (e.g., RFID tags, sensors, actuators etc), networked with each other and with other entities (including human beings) through standard communication protocols and a variety of network technologies (Atzori et al, 2010, Li et al, 2011, Lee et al, 2012). Internet of Things (IOT) adds connectivity for anything (ITU Reports, 2005) by embedding short range mobile transceivers into a wide range of gadgets and everyday objects enabling new forms of communication between people and things and between things itselves. Radio-frequency identification (RFID), sensors, miniaturization and nanotechnology are the main technologies in the upcoming environment where objects like food packages, furniture and paper documents become smart having the ability to communicate and interact (Kosmatos et al, 2011). A smart item can be tracked through space and time throughout its lifetime, can be uniquely identifiable, and characteristics as its location, temperature, and movement can be recorded. This real time monitoring allows the mapping of the real world into the corresponding virtual world (Atzori et al, 2010) where essential information about a person can be recovered by recovering data contained in smart objects around him. Sterling (2010) coined the term spime as an object that can be traced through space and time, from the time before it was made (its virtual representation), through its manufacture, its ownership history, its location until its eventual obsolescence and breaking down back into raw material.

The growing role of digital evidence to support conventional criminal evidence also illustrates the need for law enforcement agencies to adopt new investigation methods. Up to now, most investigation models deal with only physical or only digital evidence, thus imposing a clear separation. For example U.S. National Institute of Justice (2000) manual about the crime scene investigation and Lee's ***et al.*** (2001) Scientific Crime Scene Investigation Model do not include specifications about digital evidence and their role in the documentation of a case. Even the U.S. National Institute of Justice Special Report for electronic crime scene investigation (2008), focuses mainly on procedures concerning digital devices and not on the interpretation of the data they contain. On the other hand, state-of-the-art digital forensic models do not sufficiently pay much attention to physical evidence which is also very important for a case. (Palmer, 2001; Carrier and Spafford, 2003; Ciardjuain, 2004; Rogers *et al.*, 2006; Agarwal *et al.*, 2011; Yusoff *et al.*, 2011).

We believe there is often a constant interaction between digital and physical evidence in a crime scene and novel investigation strategies should be pursued, aiming to avoid the loss of crucial evidence, physical or digital. For example, if an operating computer is used only as a source of physical evidence (for example fingerprints), there is the danger of losing volatile data or terminating a running process by an accidental move of the mouse or a keystroke. On the other hand if a computer is faced only as a source of digital evidence it is possible to miss physical evidence like fingerprints and DNA which could be collected from the surface or the internal of a computer or peripheral device. Furthermore, various items found in a crime scene may worth be examined as both physical and digital evidence *e.g.*, a printed paper can be related to a specific printer or a file stored in a hard disk or flash memory, a piece of clothes may have an embedded system-on-chip (SOC) and a wall clock could also be a part of a surveillance system as it contains a hidden micro camera. As noted before, many physical everyday objects in a smart environment may have embedded digital equipment and even be interconnected. This evolution requires law-enforcement agencies to be *digital ready* and use a combination of physical and digital forensics methods and techniques to search crime scene with such evidence.

Our Contribution. In this paper we introduce the term hybrid evidence as evidence with both physical and digital characteristics and propose a model for hybrid evidence investigation. The novelty of the proposed model is that we do not discriminate between physical and digital evidence investigation, but instead we consider all evidence types potentially present in most crime investigations. Our model extends the traditional physical crime scene investigation models which law enforcement agencies use for decades to incorporate the digital environment. An important feature of the model is that it can also be used in crime scenes where only digital or physical evidence exist. In addition, we validate the usefulness of our model by discussing a detailed case example of an imaginary investigation where our model is applied. This paper extends the work done in (Vlachopoulos et al, 2012).

2. Related work

Crime investigation theory remains an open field of research as offenders find new ways to commit crimes. In law enforcement investigations, commonly accepted procedures are implemented by most agencies around the world. For instance a typical investigation includes the following basic steps (Vlachopoulos, 2007): Police are notified about a crime; after the necessary preparation an investigation takes place at the crime scene; the scene is secured, a thorough search for evidence is contacted and items considered as evidence are documented, bagged, labeled, collected and transported to the lab for further examination; finally a police report refers to the results of the investigation.

The majority of models that have been presented so far for physical crime scene investigations include a number of common steps. For example, the U.S. National Institute of Justice report on Crime Scene Investigation (2008) includes nine top level steps: a. Preparation, b. Preservation, c. Preliminary Documentation and

Evaluation of the scene, d. Documentation, e. Collection, f. Preservation, g. Package, h. Transport, i. Report. These steps are met in most investigation models.

Lee *et al*. (2001) presented the *Scientific Crime Scene Investigation Model*, which focuses on a systematic and methodical way of investigating a physical crime scene. The model consists of four stages:

1. **Recognition:** In this stage, items or patterns which are found in the crime scene are noticed as potential evidence.

2. **Identification:** Items found in the crime scene are recognized as evidence and classified into physical, biological, chemical or other form of evidence. A comparison with known standards of evidence is also conducted.

3. **Individualization:** In this stage the uniqueness of possible evidence is examined in order to link evidence to a particular individual or event.

4. **Reconstruction:** The outputs of the previous stages and the evaluation of any other relevant information leads to a detailed report about the events and actions at the crime scene.

Although the model refers only to physical crime scene investigation, it became a point of reference as many of its aspects can be used to search for digital evidence in an electronic crime scene investigation. The model refers only to the forensic part of an investigation, while issues such as preparation and exchange of information with other investigators are not addressed.

In the *Digital Forensic Research Workshop* (Palmer, 2001), a digital forensic investigation model was suggested which includes a set of seven steps derived from a number of actions that have to be performed in each step:

1. **Identification:** Event/Crime Detection, Resolve Signature, Profile Detection, Anomalous Detection, Complaints, System monitoring, Audit Analysis etc.

2. **Preservation:** Case management, Imaging Technologies, Chain of Custody, Time Synch

3. **Collection:** Preservation, Approved Methods, Approved Software, Approved Hardware, Legal Authority, Lossless Compression, Sampling, Data Reduction, Recovery Techniques

4. **Examination:** Preservation, Traceability, Validation Techniques, Filtering Techniques, Pattern Matching, Hidden Data Discovery, Hidden Data Extraction

5. **Analysis:** Preservation, Traceability, Statistical, Protocols, Data Mining, Timeline, Link, Special

6. **Presentation:** Documentation, Expert Testimony, Clarification, Mission Impact Statement, Recommended Countermeasure, Statistical Interpretation

7. **Decision**

The aim of the model was to set the basis for future work which would define a full model. It became a point of reference in the coming years as its steps are included in most of the recent models. The model cannot be used directly in a real investigation as it does not include a comprehensive explanation of the actions that have to be performed in each step but only a list of overlapping techniques.

Carrier and Spafford (2003) suggested a digital investigation process, which includes both physical and digital evidence investigation in one integrated process. The model consists of seventeen phases organized into five groups:

1. **Readiness Phases:** This group includes the Operations and Infrastructure Readiness Phases, which refer to the actions prior to an investigation such as training of the respondents and the lab analysts, as well as availability of data which are connected to an investigation

2. **Deployment Phases:** This group includes two phases a. Detection and Notification Phase and b. Confirmation and Authorization Phase. The goal is to detect and confirm that an incident has taken place.

3. **Physical Crime Scene Investigation Phases:** This group consists of six phases: a. Preservation b. Survey c. Document d. Search and Collection e. Reconstruction and d. Presentation. The goal is to collect and analyze physical evidence and identify people who are responsible for the incident.

4. **Digital Crime Scene Investigation Phases:** This group of phases is identical to the physical crime investigation phases. The goal is to search for digital evidence after the physical digital devices has been collected as physical evidence.

5. **Review:** This is a final phase of the investigation where an evaluation is conducted to identify areas of improvement.

The basic characteristic of the model is the separation of the investigation process to physical and digital crime scene investigation. Firstly, items found in the crime scene are handled as physical evidence using traditional investigation methods (*e.g.*, fingerprints). If these items are source of digital evidence (*e.g.*, computers, cellphones, peripherals) they are examined again according to digital crime scene investigation sub-phases and the results are added to the primary physical scene. The main disadvantage of this approach is that the time needed to collect physical

evidence could lead to loss of volatile data or other digital evidence related to the crime.

Ciardjuain (2004) evaluated and combined the existed models to propose the *Extended Model of Cybercrime Investigations* which consists of thirteen steps:

1. **Awareness:** This step concerns the notification that an investigation is needed. This stage is highly important because the events causing the investigation can determine the type of investigation required.

2. **Authorization:** In this step a formal authorization should be obtained to proceed to the investigation. The type of the authorization depends on the environment where the investigation is conducted.

3. **Planning:** Planning is an activity which should be carefully designed and implemented. Further problems such as the need for extra authorization and legislative restrictions can be avoided if predicted in this stage.

4. **Notification:** This step refers to informing the subject of an investigation or other concerned parties that an investigation is taking place. It can be omitted in cases where surprise is needed to prevent destruction of evidence.

5. **Search for and identify evidence:** This activity deals with locating items and identifying them as potential evidence.

6. **Collection of Evidence:** In this step the investigator collects all the evidence that can be preserved and analyzed, *e.g.*, personal computers and/or peripheral devices.

7. **Transport of Evidence:** This is a very important task because wrongful packaging and transport could affect the integrity of evidence.

8. **Storage of Evidence:** Storage is important because evidence may not be examined at once. Integrity of evidence should also be noticed.

9. **Examination of evidence:** This step requires the use of specialized techniques to find and interpret important data.

10. **Hypothesis:** In this step the investigator constructs a hypothesis of what occurred at the crime scene.

11. **Presentation:** The presentation of the hypothesis depends on the type of the investigation. For a police investigation the hypothesis will be placed before a jury, while an internal company investigation will place the hypothesis before management for a decision on action to be taken.

12. **Proof/Defense:** In this stage the investigator has to support her/his hypothesis, for example before a jury.

13. **Dissemination:** The dissemination of information is the last stage of the model and aims to use the knowledge gained from the investigation in future cases.

Unlike previous models, this model includes steps and processes before and after the crime scene investigation. The sequence of steps in the model is not absolute. Some steps can be omitted, their sequence can be modified and the results from a step can influence not only the next step but the previous one as well. The sequence of the activities described in the model could contribute to the development of new tools for digital evidence examination. The model only refers to digital evidence.

The *Computer Forensics Field Triage Process Model* (Rogers *et al.*, 2006) aims to identify, examine and interpret digital evidence as soon as the investigation begins, without the need to take the evidence to the lab for further examination. The model consists of six main phases that are further divided into another six sub-phases:

1. **Planning:** As in most forensics models, planning refers to the preparations that should be made prior to an investigation.

2. **Triage:** In the next phase, unique in this model, evidence is identified and classified according to its importance so that most important and volatile evidence can get priority to examination.

3. **User Usage Profile:** The User Usage Profile phase and its sub-phases (a. Home, b. File properties, c. Registry) concentrate on user's activity and how any observed activity can be connected to a particular user.

4. **Chronology Timeline:** At this phase, the case is been examined from chronological perspective, in order to determine the chronological sequence of the crime events, using for example Modification, Access and Creation (MAC) Time of files.

5. **Internet:** Internet is the next phase where the investigator examines internet services (e.g., Browser, e-mail, IM).

6. **Case Specific:** Finally, the investigator can adjust the focus of the examination to the specifics of the case *e.g.,* investigating child pornography is different than investigating drug activities or financial crimes.

The model focuses on the need to collect as much evidence as possible, immediately after the investigation begins as in many cases immediate action is required to resolve the crime. The model also focuses on the specifics of each case. This feature limits the model's value since it can be used only in a limited number of cases.

Furthermore, the format of the model resembles to a computer-based or network-based forensic model, where physical evidence is totally ignored.

The *Systematic Digital Forensic Investigation Model* (Agarwal *et al.*, 2011) includes eleven stages which are similar to the ones that had been suggested in previous models, except the evidence collection stage which is divided into Volatile Evidence and Non-Volatile Evidence Collection sub-phases:

1. **Preparation:** It involves an initial understanding of the nature of the crime and preparation of materials for packing evidence sources etc.

2. **Securing the Scene:** It includes the protection of the crime scene for unauthorized access and preserving evidence for being contaminated.

3. **Survey and Recognition:** This stage involves an initial search for evaluating the crime scene, identifying potential evidence and formulating a search plan.

4. **Documenting the Scene:** The documentation of the crime scene includes a number of tasks like photographing, sketching, and mapping.

5. **Communication Shielding:** This is a step prior to collecting evidence where it must be ensured that all communications features of digital devices are disabled.

6. **Evidence Collection:** In this step evidence located at the crime scene has to be collected ensuring its admissibility in a court of law. The collection of evidence is separated to Volatile Evidence Collection and Non-volatile evidence Collection.

7. **Preservation:** This phase includes packaging, transportation and storage.

8. **Examination:** Collected evidence should be examined by forensic experts to extract critical information about the case. The examination includes the use of a number of tools and techniques for analyzing data.

9. **Analysis:** The results of the examination are analyzed in this phase to identify relationships between data, determine the significance of the information obtained etc.

10. **Presentation:** In this stage the results of the previous steps are presented before a wide variety of audience including law enforcement officials, technical and legal experts etc.

11. **Result:** This is the last step of the model where a review of all the steps of the investigation is conducted in order to locate areas of improvement.

It is a comprehensive model, targeting computer frauds and cyber crimes investigations. Basically, the model ignores the physical nature of evidence. Only the Non-volatile evidence collection sub-phase considers evidence of non-digital nature such as written passwords, hardware and software manuals, related documents and computer printouts. Critical physical evidence like fingerprints or DNA which could be found on the surface or the internal of the devices placed at the crime scene, are ignored.

Recently, Yusoff et al. (2011) presented an assessment on digital investigations models, from 1985 to 2011. They examined the existed models and determined their common phases. These common phases were used to make the Generic Computer Investigation Model which consists of five generic phases:

1. **Pre-Process:** Includes all the work that has to be done before the investigation like getting the necessary approval from relevant authority, preparing the tools to be used etc.

2. **Acquisition and Preservation:** This phase includes a number of activities like identification, collection, transportation, storage and preservation of data.

3. **Analysis:** This phase aims to identify the source of crime and ultimately discover the person responsible of the crime.

4. **Presentation:** This is the act of presenting the results of the analysis to the authority.

5. **Post-Process:** This is the process where the findings of the investigative process are used for improvement of future investigations

The five generic phases which are included in the model represent the main phases of each investigation in a physical or digital crime scene. Their model seems more like a framework than a model, since its phases are too general to be implemented ad-hoc in a real world investigation process.

Table 1, presents the top level phases of a selection of state-of-the-art investigation models and the target evidence of each model (physical or digital) is highlighted.

NAME OF MODEL - AUTHOR	TOP LEVEL PHASES		TARGET EVIDENCE	
			PHYSICAL	*DIGITAL*
Scientific Crime Scene Investigation Model (Lee *et al.* 2001)	1. Recognition 2. Identification	3. Individualization 4. Reconstruction	X	
The Digital Forensic Research Workshop Investigative Model (Palmer, 2001).	1. Identification 2. Preservation 3. Collection	4. Examination 5. Analysis 6. Presentation		X
An Intergraded digital investigation process (Carrier and Spafford, 2003)	1. Readiness Phases 2. Deployment Phases 3. Physical Crime Scene Investigation Phases	4. Digital Crime Scene Investigation Phases 5. Review	X	X
Extended Model of Cybercrime Investigations (Ciardjuain, 2004)	1. Awareness 2. Authorization 3. Planning 4. Notification 5. Search for and identify evidence 6. Collection	7. Transport 8. Storage 9. Examination 10. Hypothesis 11. Presentation 12. Proof / defense 13. Dissemination		X
Computer Forensics Field Triage Process Model (Rogers *et al.*, 2006)	1. Planning 2. Triage 3. User Usage Profile	4. Chronology Timeline 5. Internet 6. Case Specific		X
Systematic Digital Forensic Investigation Model (Agarwal *et al.*, 2011)	1. Preparation 2. Securing the Scene 3. Survey and Recognition 4. Documenting the Scene 5. Communication Shielding	6. Evidence Collection 7. Preservation 8. Examination 9. Analysis 10. Presentation 11. Result		X
Generic Computer Investigation Model (Yusoff *et al*, 2011)	1. Pre-Process 2. Acquisition and 3. Preservation	4. Analysis 5. Presentation 6. Post-Process	X	X

Table 1: Top level phases of crime investigation models

3. A model for hybrid evidence investigation

A criminal investigation is an official effort to uncover information about a crime and is usually conducted by law-enforcement agencies. During an investigation a number of different types of physical evidence is collected as documents, glass, soils, minerals and other vegetative matter, fingerprints, hair, fibers, firearms and ammunition, powder residue, explosives and petroleum products, impressions and tool marks, drugs, paint, blood, semen, saliva, organs and other physiological fluids. Furthermore due to the development of computers and related technologies, digital evidence has become an equal important material in many investigations. Digital evidence is data of different forms like text, images, audio and video which is stored, processed and transmitted by many digital enable devices and networks.

However the growth of digital technology is constantly changing the present and future environment and differentiates the crime investigation landscape. The *Internet of Things* is currently the leading vision which refers to this new interconnected environment. In this new environment smart objects can provide a wide range of information which can be used for crime investigation purposes. Definitely all these objects with their characteristics will play a vital role in future investigations as they are potential evidence which we refer to as *hybrid evidence* considering both their physical and digital nature. The main characteristic of such evidence is that it is not

easily identifiable because its digital nature becomes more and more invisible and there is the danger of being considered as plain physical items. For example Hitachi has developed an RFID tag with dimensions 0,4mm x 0,4mm x 0,15 mm, small enough to be embedded to tiny everyday items.

For the purposes of this paper hybrid evidence is not a new form of evidence beyond physical and digital. Actually hybrid evidence refers to both physical and digital evidence and adds the possibility of a physical object to have hidden digital characteristics which should considered in a crime investigation. These characteristics could refer to smart items as described Section 1 but also to a wide range of gadgets which become more and more popular. For example a watch, clock or pen may contain a micro camera or a microphone to record video and voice in its internal flash memory, a smoke detection device could be a home spy system, a piece of cloth, a pass card or a piece of paper might have an embedded RFID chip which contains tracking information. To this end the model proposed in this section is close to a typical law enforcement investigation model where the possibility of items having both digital and physical nature is essential.

The proposed model could be used to investigate crime scenes with hybrid evidence, but also in investigations where only digital or only physical evidence exists. The model consists of four major phases and twelve secondary sub-phases (Fig. 1).

3.1 Phase A: Preparation

(A1) Notification. This first step includes: (a) Notification that a crime has been committed. For example using European Emergency Number (112) to report a crime, sending an email, going to a police station etc. (b) Notification to the proper law enforcement agency responsible to conduct the investigation. The responsible agency can be determined by geographical criteria (location of crime scene) or the nature of the crime-incident (*e.g.*, robbery, suicide etc.). Notification is very important, because the information collected here is crucial for the next steps of the investigation.

(A2) Authorization. Authorization is obtained from the agency assigned to conduct an investigation. The form and details of the authorization depend on the type of crime and the procedural law of the country where it is committed. Typically, immediately after a crime has been discovered, assigned officers can conduct an investigation at once and inform the attorney on duty as soon as possible.

(A3) Preparation. Preparation includes availability of the necessary tools, equipment and personnel able to conduct the investigation. Preparation is important not only after the notification for a crime or incident but also before, including education and training, response, availability and functionality of tools and equipment. In this sub-phase the person responsible for the investigation is determined.

3.2 Phase B: Crime scene investigation

(B1) Preservation. The Lead first respondent at the crime scene is responsible for organizing a number of things: first aid, search for witnesses and securing the scene from people who are not authorized to approach. Additionally, possible source of physical and digital evidence should also be recognized and secured.

(B2) Identification. This is a specialized task that is preferably conducted by crime investigation experts. Their task is to identify possible evidence, physically or digitally related to items set in the crime scene. In serious crimes, the investigation could be conducted by a number of technicians specialized in different fields. Their level of cooperation and understanding is a major factor for a successful investigation. This phase also includes documentation which refers to photographing, sketching and mapping the crime scene, taking notes about items or people present at the crime scene etc.

(B3) Collection – Examination. This is one of the most important sub-phases of the model. The investigator has to collect fingerprints, items related to the crime, biological material and other physical evidence. In case there is digital evidence at the crime scene the investigator should firstly search for volatile data. In this stage the cooperation between the digital and physical crime scene experts is highly important because collection of physical evidence can destroy digital evidence and vice versa. This stage also contains examination. This is not the thorough examination procedure that is conducted in a laboratory environment. However sometimes it is important for the investigation to get as much information as soon as possible. For example in a serious crime investigation it is extremely urgent for the investigator to search the victim's mobile phone for *e.g.*, last calls or messages or a personal computer for e-mails or recent posts on social networks.

(B4) Transportation. Although transportation of evidence is usually perceived as a secondary procedure, we consider it as important as collection. During transportation special measures should be taken to avoid any damage to the evidence. Careful packaging, humidity and temperature, should be considered to avoid any destruction of physical and/or digital evidence.

3.3 Phase C: Laboratory examination

(C1) Examination. The examination of evidence in a laboratory environment is essential to any investigation because it can provide the investigator with crucial evidence related to the case. While at the crime scene only a part of the collected evidence can be examined, in this phase all evidence is thoroughly examined and analyzed according to the nature of evidence and the specifics of each case.

(C2) Storage. After examination, evidence should be stored properly in a locked evidence room with stringent access controls. The evidence should be labeled and segregated to avoid any cross contamination, to avoid destruction and to enable re-examination if such need occurs in a court or any other step of the investigation.

(C3) Report. The Report determines the outcome of the laboratory examination phase. The report of the lab is one of the most important documents for the investigator and all parties involved in a case (prosecution and defence).

3.4 Phase D: Conclusion

(D1) Reconstruction. Crime reconstruction is the main responsibility of the investigator who evaluates the collected and examined evidence and represents the facts as defined by the evidence analysis. This step is only of value if the previous steps have been followed forensically such that anyone following the same method would arrive at the same results.

(D2) Dissemination. Dissemination is the last step of the model. A thorough review of the investigation is conducted in this step to preserve gained knowledge and identify areas of improvement. Lessons learned should be carefully recorded and disseminated to other parties which conduct similar investigations.

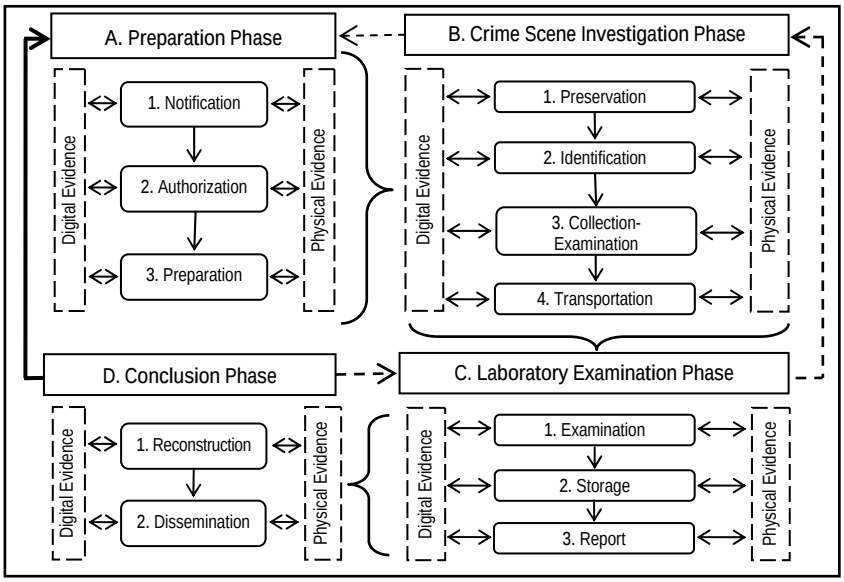

Figure 1: A model for hybrid evidence investigation

3.5 Model Analysis

The proposed model for hybrid evidence investigation holds the majority of the benefits of the existing models adding an extra advantage: It can be implemented to every crime scene investigation whether digital evidence is present or not. The format of the model resembles a traditional law enforcement investigation model, but it has been adjusted to also face the challenges of digital evidence and the emergent technologies. The model can be easily interpreted, because it is divided into specified phases and a number of sub-phases. This is very important for the investigators who

are called to practice it but also for the trainers who teach crime investigation methods and techniques.

The model examines the whole process of crime investigation, starting from the notification that a crime has been committed, ending to the findings of the research. Digital and physical evidence are equally important and influence every sub-phase of the model (double arrows in Fig. 1). Phase B targets the search and collection of physical and digital evidence, which are in constant interrelation. In this phase, the collection-examination sub-phase is highly important. In the collection sub-phase, there is not a defined order in evidence collection. The investigator is responsible to take a critical decision and determine if volatile and other digital data should have priority over collection of physical evidence such as fingerprints or biological material. The examination sub-phase at the crime scene does not intend to replace the laboratory examination but to help the investigator to collect important evidence crucial for the next steps as soon as the investigation begins. Digital evidence seems to mostly affect this phase; however its role is highly important to all phases of the model. For example, in Phase A, the existence of digital evidence affects the type of authorization needed and the personnel who will conduct the investigation. Unlike previous models, laboratory examination of the collected evidence from the crime scene is a separate and very important phase.

Although there is a defined order in the phases of the model, iteration at each phase or returning to a previous phase is also an option. Inarguably an investigation is a process where a number of unpredictable factors can occur. Returning to a previous phase (marked in Fig. 1 with dotted arrows) could help the investigator to fill in the gaps and ensure that all evidence is adequately collected and analyzed. After the investigation ends, the knowledge gained may be used as feedback to improve the investigation process (straight bold line in Fig. 1) so that lessons learned can be considered in future investigations.

As in every model for law enforcement investigations the responsibility of the investigation belongs to the assigned investigator. He/she is in charge of all the aspects of the investigation, guides experts of other fields who participate in the investigation process and in Phase D he/she draws conclusions about the investigation. Despite the key role of the investigator other people are also involved in the investigation process. For example in Phase A emergency call first responders should collect all the necessary information and report to the proper agency as soon as possible. In Phase B first responders have to secure the crime scene while forensic experts of different fields have to collect and examine primary evidence, possibly of different types, and, finally, in Phase C collected and transported evidence is examined in a laboratory environment by specialized personnel.

4. Case example: Implementing the proposed model in a house investigation

In many investigations a house is a place where the need to search for important evidence often occurs. A house may be the primary crime scene or a secondary scene

which should be investigated to find valuable evidence that can be linked to a person or object. In order to show, at a high level, how our model could be implemented in an investigation we examined an imaginary drug case as follows: A person is arrested in a typical police patrol near his apartment as he was found in the possession of drugs. He is brought to the police station and identified as John Doe. His apartment is decided to be searched for extra evidence. This is a sample mapping of the actions that have to be performed according to the proposed model for hybrid evidence investigation:

Phase A: Preparation. The ***Notification*** occurs when John in arrested and the incident is reported to the police headquarters. ***Authorization*** refers to the search warrant which was acquired in order to conduct the house investigation. In the **Preparation** sub-phase, a team which consists of the investigator in charge, a physical and a digital crime scene expert is being prepared to conduct the investigation. The members of the team are fully trained and equipped with the necessary tools, equipment and software.

Phase B: Crime Scene Investigation: In ***Preservation*** sub-phase**,** the team arrives at the apartment which is considered as crime scene and designates a perimeter in order to prevent unauthorized access. The next step is ***Identification***. Before entering the apartment the digital expert investigator uses technological equipment and software in search of a sensor system which may be enabled when the door opens. Also the physical crime scene expert searches the door for fingerprints. Fingerprints are found and collected where there is no sensor system. The door of the apartment opens using a smart card provided by John. A first look inside the apartment is taken along with some photographs of the crime scene and the following items are identified**: i) personal computer (PC), ii) office with a chair, iii) A wooden box iv) a printed paper v) a pen**. The physical crime scene investigator maps the crime scene and takes notes about items found, while the digital investigator approaches the PC for a closer examination. The PC is turned on and he decides not to switch off the cable modem at once because an incoming e-mail is still downloaded. He switches the modem off after the download has been completed. Before touching the mouse and keyboard he asks the physical crime scene investigator to search them for fingerprints without moving the mouse in case there is a sensor system or pressing a key on the keyboard which could alter the data. The physical investigator also checks the office and chair for fingerprints or other physical evidence; he collects fingerprints from the desk and biological material (hair) from the chair and allows the digital investigator to continue with volatile data collection. The digital investigator collects volatile data according to digital forensic standards and turns off the PC by pulling the plug. The ***Collection-examination*** sub-phase is in progress. The physical investigator searches the rest of the objects identified for physical evidence. He realizes that in the wooden box there is small portion of powder possibly remaining of a drug substance. Before collecting and packaging the box the digital investigator also examines it on site. It does not seem to have any digital characteristics but after scanning it with special equipment he finds out that there is an embedded chip which records location information about the box. He recovers this information and gives them to the investigator in order to examine the movements of the box, who and when sent it etc. The printed paper contains a list of

six names with their addresses and telephones. The physical crime scene expert notes them down and gives them to the investigator. The digital expert examines the paper and he realizes that it was printed probably recently in an inkjet printer. He collects the paper to be sent to the laboratory in case the printed paper can be related to a file stored in the PC or the source printer. Finally the pen is examined for fingerprints but the digital crime scene expert realizes that it contains a hidden micro camera and an embedded 8 GB flash memory . He collects it to send it to the lab for further examination. All the objects found at the crime scene are collected and packaged according to their nature. Physical items with digital characteristics are packaged in such way to avoid cross-contamination from networking devices, local electricity, humidity etc. For example the box is collected and labeled with the notification that it contains an embedded chip which should also be examined for digital evidence and is placed in an antistatic bag to avoid contamination. **Transportation** of collected objects to the lab is the last step of this phase. A careful packaging is essential for safe transformation.

Phase C: Laboratory Examination: In the ***Examination*** sub-phase, all items collected from the crime scene are examined in the forensic laboratory in search of additional evidence which could help the investigator to link/trace persons and things. Each item is carefully checked for both digital and physical evidence and priority to examinations is decided. After examination has been completed all objects are properly stored in order to be examined again if such need occurs in the future. **Storage** is essential because examined items may be kept in a warehouse for a long time so the necessary precautions are taken to protect them from temperature, humidity or other cross-contamination. Finally in the **Report** sub-phase the lab prepares a report with the results of the examination and gives it to the investigator for his further actions. In this report it is noted that in PC's hard drive a file similar to the printed paper was found. The file was sent at Johns e-mail by a person called Joe Shmoe. The wooden box contains a microchip with historical information about the box including weight and location. A file with this information was also recovered from the hard drive. The pen contains videos filmed in the apartment and outside, where John talks to three different people about drug deals.

Phase D: Conclusion: In the **Reconstruction** phase the investigator puts together all the pieces of the case and reaches to his conclusions. The case has as follows. John is a drug dealer. He contacts Joe via e-mail, where Joe is the major drug dealer. Joe sends drugs to John using the wooden box, which contains a chip which records tracking information. The box is sent to John from various locations using courier services, so the chip helps them to track the movements of the box during its transportation. Log files containing the movements of the box where found in John's PC. The people on the list are candidate buyers. Joe sent the list to John by e-mail in a word file which was found stored in John's PC. John meets the candidate buyers and uses the pen with the hidden micro camera to record the drug transaction. The videos recovered by the pen's memory and many others found stored in the hard drive shows several meetings probably with the people contained in the list. The fingerprints found at John's apartment belong to him, while the DNA analysis showed that the hair found in the chair belongs to Joe. After all this evidence Joe is also arrested while the people in the list are suspects involved in the case as drug

users. Finally in the **Dissemination** sub-phase, the modus operandi of John and Joe and lessons learned from the whole investigation process is valuable information which will be documented and saved for future reference.

This is a sample case, actually a part of a full case that shows how digital evidence can influence every case under investigation. Definitely in a future investigation conducted in a full operated IOT environment, the hybrid element will be essential and the apartment of our case example could be considered as a hybrid crime scene. Although our model does not propose a clear solution of how all these evidence should be collected, it illustrates the need to keep in mind that the digital element exists *anytime*, *anyplace* for *anyone* and *anything*. Finally this case example shows that the level of co-operation between the physical and the digital expert is very important.

5. Conclusions

In this paper, we considered crime scene investigation where digital and physical evidence may co-exist, and presented the key challenges of law enforcement investigation in the new environment. Additionally, we reviewed a selection of investigation models for physical/digital evidence, we introduced the term hybrid evidence and proposed a model for hybrid evidence investigation. We also discussed a detailed example of an imaginary crime investigation where our model is applied. Our model unifies the procedures related to digital and physical evidence collection and examination, taking into consideration the unique characteristics of each form of evidence. Inarguably, the proposed model is still in its infancy. It should be tested and evaluated in real investigation environments and get feedback which would define the necessary modifications. Additionally, a more detailed description of each phase of the model is needed, also supported by a manual for investigators which should include further technical instructions related to an investigation. These are left for future work.

6. References

Agarwal, A., Gupta, M., Gupta, S. and Gupta S.C. (2011), "Systematic Digital Forensic Investigation Model", *International Journal of Computer Science and Security*, Vol. 5, No. 1, pp 118-131.

Atzori, L., Iera, A. and Morabito, G. (2010) "The Internet of Things: A survey," *Computer Networks*, Vol. 54, No. 15, pp. 2787-2805.

Beebe, N. (2009), "Digital Forensic Research: The Good, The Bad, and The Unaddressed," in Advances in Digital Forensics V, Peterson G. and Shenoi S. (eds.), Boston, Springer, pp 17-33. ISBN 978-3-642-04154-9.

Carrier, B. and Spafford, E. (2003), "Getting Physical with the Digital Investigation Process, *International Journal of Digital Evidence*, Vol. 2, No. 2.

Ciardhuain, S. (2004), "An Extended Model of Cybercrime Investigations", *International Journal of Digital Evidence*, Vol. 3, No. 1.

Garfinkel, S. (2010), “Digital Forensics Research: The next 10 years”, *Digital Investigation*, Vol. 7, pp S64-S73.

Hunton, P. (2010), “Cyber Crime and Security: A New Model of Law Enforcement Investigation”, *Policing,* Vol. 4, No. 4, pp. 385-395.

Hunton, P. (2011), “The stages of Cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation”, *Computer law and Security Review*, Vol. 27, No. 1, pp. 61-67.

Kosmatos, E., Tselikas, N. and Boucouvalas, C. (2011) “Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture”, *Advances in Internet of the Things*, Vol. 1 No. 1, pp. 5-12.

Lee, H., Palmbach, T., and Miller, M. (2001), *Henry Lee’s Crime Scene Handbook*, Academic Press, San Diego, ISBN: 0-12-440830-3.

Lee, I., Sokolsky, O., Chen, S., Hatcliff, J., Jee, E., Kim, B., King, A.L., Mullen-Fortino, M., Park, S., Roederer, A., Venkatasubramanian, K.K.: Challenges and research directions in medical cyber-physical systems. Proceedings of the IEEE 100(1), 75-90 (2012)

Li, X., Lu, R., Liang, X., Shen, X., Chen, J., Lin, X.: Smart community: an Internet of Things application. Communications Magazine, IEEE 49(11), 68-75 (2011)

National Institute of Justice (2000), “Crime Scene Investigation, A guide for law enforcement”, Research Report, *U.S. Department of Justice,* https://www.ncjrs.gov/pdffiles1/nij/178280.pdf, (Accessed 27 January 2012).

National Institute of Justice (2004), “Forensic Examination of Digital Evidence: A Guide for Law Enforcement”, Special Report, *U.S. Department of Justice, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf,* (Accessed 27 January 2012).

National Institute of Justice (2008), “Electronic Crime Scene Investigation. A Guide for first Respondents”, Special Report, Second Edition, *U.S. Department of Justice* https://www.ncjrs.gov/pdffiles1/nij/219941.pdf, (Accessed 27 January 2012).

Palmer, G. (ed.), (2001), “A Road Map for Digital Forensic Research”, Digital Forensic Research Workshop (DFRWS) Technical Report DTR-T001-01, Utica, New York, http://www.dfrws.org/2001/dfrws-rm-final.pdf, (Accessed 27 January 2012).

Palmer, G. (2002), “Forensic Analysis in the Digital World”, *International Journal of Digital Evidence*, Vol. 1, No. 1.

Reith, M., Car, C., and Gunsch, G. (2002), “An Examination of Digital Forensic Models”, *International Journal of Digital Evidence*, Vol. 1, No. 3.

Rogers M., Goldman J., Mislan R., Wedge T. and Debrota S. (2006), “Computer Forensic Field Triage Process Model”, *Journal of Digital Forensics, Security and Law*, Vol. 1, No. 2, pp 19-38.

Sheldon, A. (2005), “The future of forensic computing”, *Digital Investigation*, Vol. 2, pp 31-35.

Sterling, B. (2005), “Shaping Things–Mediawork Pamphlets”, *The MIT Press*

Vlachopoulos, K. (2007). *Electronic Crime*, Nomiki Vivliothiki, Athens, ISBN: 978-960-272-458-3.

Vlachopoulos, K., Magkos, E., and Chrissikopoulos, V. (2012), "A Model for Hybrid Evidence Investigation", Proceedings of 7th International Annual Workshop on Digital Forensics & Incident Analysis (WDFIA 2012).

Yussof, Y., Ismail, R., and Hassan Z. (2011), "Common Phases of Computer Forensics Investigation Models", *International Journal of Computer Science & Information Technology*, Vol. 3, No. 3, pp 17-31.